

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

6403 KENNEDY AVE., APT. 3
CINCINNATI, OHIO 45213

Case No. 1:21-mj-700

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description


18 U.S.C. 1001

Making False, Fictitious, or Fraudulent Statement or Representation.

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

William Crayner, Special Agent, ATF&E

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

via FaceTime video

(specify reliable means)

Date: **Oct 1, 2021**

City and state: Cincinnati, Ohio


Karen L. Litkovitz
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is 6403 KENNEDY AVE., APT. 3, CINCINNATI, OH 45213, The apartment building is a four-family building. Apartment 3 is located on the top floor on the south side of the building. It can be seen and identified from the street as the top left apartment from the front door. It is a red brick building with dark colored siding on the top floor. The numbers “6403” are on the front door in light colored numbers.



ATTACHMENT B

Property to be seized

1. All communications, in whatever form they may be—whether they are audio recordings, electronic communications, or otherwise—that contain evidence of Shamika HEIDELBERG’s contacts and communications with David BRYERS from September 1, 2021 to present.

2. All cellphones, mobile phones, and smartphones belonging to or used by BRYERS or HEIDELBERG (hereafter, any “Phone”), including but not limited to the (513) 354-9529 Phone and the (513) 648-4379 Phone;

3. To the extent contained on any Phone seized from the PREMISES, all records relating to violations of 18 U.S.C. § 1001, a violation involving David BRYERS and/or Shamika HEIDELBERG and occurring on or about September 28, 2021, through the present, including records and information relating to:

- a. Communications between BRYERS and HEIDELBERG related to obstructing, impeding, interfering, or influencing the investigation and judicial proceedings regarding BRYERS’ federal arrest warrant and/or wanted status.
- b. Communications from BRYERS and/or HEIDELBERG to third parties related to obstructing, impeding, interfering, or influencing the investigation and judicial proceedings regarding BRYERS’ federal arrest warrant and/or wanted status.
- c. Evidence indicating how and when the Phone was accessed or used, to determine the chronological and geographic context of access and use as it relates to the crime under investigation and the Phone’s user;

- d. Evidence indicating the Phone user's state of mind as it relates to the crime under investigation; and
 - e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.
4. For any Phone whose seizure is otherwise authorized by this warrant:
- a. evidence of who used, owned, or controlled the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the Phone was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the Phone user;
 - e. evidence indicating the Phone user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the Phone of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Phone;

- h. evidence of the times the Phone was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the Phone;
 - j. documentation and manuals that may be necessary to access the Phone or to conduct a forensic examination of the Phone;
 - k. records of or information about Internet Protocol addresses used by the Phone;
 - l. records of or information about the Phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
5. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:
6403 KENNEDY AVE., APT. 3,
CINCINNATI, OHIO 45213

Case No. 1:21-mj-700

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, William Crayner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6403 KENNEDY AVE., APT. 3, CINCINNATI, OHIO 45213 (the “**SUBJECT PREMISE**”), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent (“SA”) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”), and have been so employed since December 2018. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Glynco, Georgia. I also graduated from the ATF Special Agent Basic Training Academy, located in Glynco, Georgia, in June of 2019.

3. In my career with ATF, I have been assigned to the Cincinnati Field Office in the Southern Judicial District of Ohio. Prior to my employment with ATF, I was a member of the United States Secret Service in Washington D.C. where I served as a member of the Uniformed Division under the Presidential Protective Division. I was employed in that capacity from July of 2010 to February of 2015. I was also a member of the Carmel Police Department in Carmel, IN from February 2015 to December of 2018. I was assigned to the Operations Division at the Carmel

Police Department and took part in various criminal investigations during my tenure. I have received additional training in several areas of law enforcement, including but not limited to gang investigations, narcotics interdiction and investigation, and firearms interdiction and investigation. I am also a graduate of Purdue University where I received a bachelor's degree in Law and Society in 2008.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. I believe that below stated facts will provide probable cause of violations of 18 U.S.C. § 1001, Making False, Fictitious, or Fraudulent Statement or Representation.

PROBABLE CAUSE

A. On September 22, 2021, David BRYERS was indicted by a federal Grand Jury in the Southern District of Ohio.

6. On September 22, 2021, a federal Grand Jury in the Southern District of Ohio returned an Indictment charging David BREYERS with 18 U.S.C. § 922(u) – Theft of Firearms from a Federal Firearms Licensee and 18 U.S.C. § 922(g)(1) – Possession of Firearms by a Prohibited Person. I received an arrest warrant in case 1:21-CR-101 filed through the United States District Court for the Southern District of Ohio.

B. In September 2021, I identified 6403 Kennedy Ave, Apt. 3, Cincinnati, OH 45213 as a known address for BRYERS.

7. On September 13, 2021, I saw a black Toyota Avalon, bearing Ohio plate: JEF3804 drive down the driveway of 6403 Kennedy Avenue, the **SUBJECT PREMISE**. This vehicle is

owned by Shamika HEIDELBERG. I saw HEIDELBERG driving the Toyota and a male in the front passenger seat, matching BRYERS' description. I visually confirmed that BRYERS was the male in the front passenger seat. On September 27, 2021, I met with a representative of Cincy Sites, LLC (hereinafter "the Property Owner"), who owns 6403 Kennedy Avenue, Apt. 3, Cincinnati, Ohio 45213, the **SUBJECT PREMISE**. I asked the Property Owner about the property and the Property Owner said that Shamika HEIDELBERG is on the lease as residing at Apartment 3. The Property Owner provided me with HEIDELBERG's phone number: (513) 354-9529. The Property Owner also said that he has seen BRYERS in the apartment several times throughout the past six to eight months and believed he may have his own key to Apartment 3. The information provided to me by the Property Owner, corroborated my own observations.

C. On September 28, 2021, the Cincinnati Police Department (CPD) and ATF Cincinnati Field Office responded to the SUBJECT PREMISE and made contact with HEIDELBERG.

8. On September 28, 2021, at approximately 6:30 a.m., the ATF Cincinnati Field Office and the CPD responded to the **SUBJECT PREMISE**, the address associated with BRYERS as described above, to attempt to locate BRYERS to affect his active arrest warrant.

9. Law enforcement knocked and announced their presence on the front door of Apartment 3 (**SUBJECT PREMISE**), which is located on the top floor of the building. A woman, who identified herself as Shamika HEIDELBERG, opened the door. HEIDELBERG is the known lease holder at the apartment. HEILDELBERG stated that BRYERS was not at the apartment and consented to law enforcement searching the apartment for BRYERS. BRYERS was not located within the residence.

10. I spoke with HEIDELBERG in the hallway outside of the apartment. I was wearing overt police markings and identified myself as an ATF Agent. I further advised HEIDELBERG that BRYERS had an active arrest warrant and that I needed to locate him. HEIDELBERG stated that she had broken up with BRYERS a few weeks ago and she stated that he was not coming around her apartment anymore. I asked HEIDELBERG if she had any way of contacting BRYERS, through the phone, or any social media accounts. HEIDELBERG said she did not have any way of contacting BRYERS. I then asked HEIDELBERG if she knew of any locations where BRYERS would be staying, living, or hanging out. HEIDELBERG stated she did not know of any locations where BRYERS could be located. HEIDELBERG stated that BRYERS hung out with “weird” people and that he was frequently at locations that she did not know about.

11. I wrote my government provided cell phone number in a notebook provided by HEIDELBERG and asked her to call me at that number if she saw BRYERS or learned of any information relating to his whereabouts, and to provide me with such information. After speaking with HEIDELBERG, all law enforcement then left the location.

12. Throughout the entirety of September 28, 2021, I provided only HEIDELBERG with my government provided cell phone number and she was the sole occupant of her apartment while law enforcement was on scene. I did not provide any other individuals my government cell number on that date. I also never made contact or attempted to contact anyone else regarding BRYERS’ arrest warrant or his whereabouts. I did not tell any other known associates of BRYERS that BRYERS had an active arrest warrant. Therefore, I believe that HEIDELBERG is the only close associate to BRYERS who has my government provided cell number and the only close associate who learned of BRYERS arrest warrant from law enforcement.

D. On September 28, 2021, at 2:27 p.m., I received an incoming phone call from BRYERS.

13. On September 28, 2021, at 2:27 p.m., I received an incoming phone call on my government provided cell phone from phone number (513) 658-4379. I answered and an unknown male voice, identified himself as “David Bryers.” The male on the phone then stated that he had heard I was looking for him. I asked the male how he knew that, and he told me that he called around and got my information from the “clerk of courts.” The male further elaborated that the clerk of courts told him that he had a federal case. I asked BRYERS if Shamika gave him my phone number and he stated that he got my number from “calling around.”

14. I told BRYERS that I needed to speak with him regarding an incident that took place in May 2020. BRYERS asked about specifics of my investigation, and I told him that I would not conduct an interview over the phone and that I needed to speak with him in person at the federal building in downtown Cincinnati. BRYERS stated that he would be willing to come to the federal building and talk and that he would be available between 5:00 p.m. and 6:00 p.m. that same day. I told BRYERS that I was available during that time and that I would see him then.

15. At 5:07 p.m., I received another incoming phone call on my government provided cell phone from David Singleton using number (513) 543-7254, who identified himself as BRYERS’ attorney. I told Mr. Singleton that BRYERS had an active arrest warrant and we discussed BRYERS turning himself in; Mr. Singleton told me that BRYERS would turn himself in at approximately 6:00 p.m. At 5:59 p.m., Mr. Singleton called me and told me BRYERS would turn himself in at 9:00 a.m. the following morning.

E. On September 29, 2021, BRYERS is a no-show at the federal building, 550 Main Street, Cincinnati, Ohio 45202.

16. I arrived at the federal building at approximately 8:45 a.m., along with ATF Task Force Officer Jason Wharton. TFO Wharton and I arrived on the main floor lobby of the federal building to await BRYERS' arrival. At 9:00 a.m., BRYERS was not at the federal building as instructed.

17. At 9:11 a.m., I sent an iMessage to Mr. Singleton's phone number and asked where BRYERS was, as BRYERS had not arrived as scheduled. Mr. Singleton responded that he would see what he could find out about BRYERS' whereabouts. I never received any information about BRYERS' whereabouts from Singleton, or anyone else, and BRYERS did not turn himself in at 9:00 a.m.

18. At 9:28 a.m., I called the number (513) 658-4379, that BRYERS had called me from the previous day. The phone call was immediately directed to a voicemail, indicating the device for the number was turned off. The automated voice stated that a voicemail box for that number had not been set up, so I was unable to leave a voice message. I hung up and immediately called the number again, to confirm that the first phone call went through properly. I received the same message from the first attempt.

19. At 10:02 a.m., I sent Mr. Singleton an iMessage that BRYERS could turn himself in at the United States Marshals Office, or any police district in the country. To date, BRYERS has not turned himself in to law enforcement.

20. Based on my training and experience, I believe there is probable cause that HEIDELBERG made a knowing false statement to a federal law enforcement agent and evidence of a violation of 18 U.S.C. § 1001 will be located in the **SUBJECT PREMISE**. Based on my

training and experience, I believe HEIDELBERG's statement that she did not have any way to contact BRYERS was false and that HEIDELBERG contacted BRYERS following our interaction on September 28, 2021, at the **SUBJECT PREMISE**. My belief is based on my knowledge that BRYERS and HEIDELBERG have had an established relationship, which spanned over several months. As explained above, I saw BRYERS and HEIDELBERG together approximately two weeks prior to my conversation with HEIDELBERG. The Property Owner established that BRYERS was at HEIDELBERG's apartment frequently over the past six to eight months. I also provided my cell phone number to HEIDELBERG and her alone. I then received a phone call from BRYERS asking about my investigation approximately eight hours later and BRYERS would not elaborate as to where he obtained my phone number other than the clerk of courts provided it to him. I contacted both the Hamilton County (OH) Clerk of Courts and the Clerk of Courts for the Southern District of Ohio. Both offices stated they did not have my cell phone number to provide to anyone and if they did, that is not their common practice. Therefore, I believe that HEIDELBERG contacted BRYERS and gave BRYERS my government cell number after I spoke to HEIDELBERG.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described above and in Attachment B, this application seeks, among other things, permission to search for cellphones, mobile phones, and smart phones (all forms of computers and/or storage media) that might be found on the **SUBJECT PREMISE**, as well as relevant records and information that might be stored on those devices. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. *Probable cause.* I submit that if a cellphone, mobile phone, or smart phone is found on the **SUBJECT PREMISE**, there is probable cause to believe that relevant records will be stored on that device for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to, among other things, locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers (including cellphones, mobile phones, and smartphones) were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISE** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide

crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it

requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

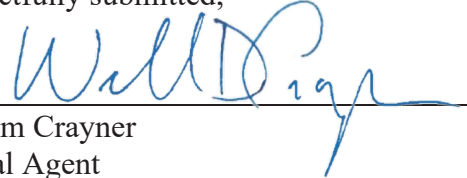
26. I submit that this affidavit supports probable cause for a warrant to search the **SUBJECT PREMISE** described in Attachment A and seize the items described in Attachment B, all in violation of 18 U.S.C. § 1001.

REQUEST FOR SEALING

27. I respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation. The targets of this investigation, BRYERS and HEIDELBERG, are not aware of the full scope of the government's attempts to obtain evidence in this case. If BRYERS and HEIDELBERG learn that the government continues to investigate, and in particular if they learn of the government's intent to search HEIDELBERG's residence, BRYERS may direct HEIDELBERG to dispose of the evidence sought by this search warrant, or

other evidence about which the government is not yet aware. For these reasons, premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



William Crayner
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1
this 1st day of October, 2021.



Karen L. Litkovitz
United States Magistrate Judge



ATTACHMENT A

Property to be searched

The property to be searched is 6403 KENNEDY AVE., APT. 3, CINCINNATI, OH 45213, The apartment building is a four-family building. Apartment 3 is located on the top floor on the south side of the building. It can be seen and identified from the street as the top left apartment from the front door. It is a red brick building with dark colored siding on the top floor. The numbers “6403” are on the front door in light colored numbers.



ATTACHMENT B

Property to be seized

1. All communications, in whatever form they may be—whether they are audio recordings, electronic communications, or otherwise—that contain evidence of Shamika HEIDELBERG’s contacts and communications with David BRYERS from September 1, 2021 to present.

2. All cellphones, mobile phones, and smartphones belonging to or used by BRYERS or HEIDELBERG (hereafter, any “Phone”), including but not limited to the (513) 354-9529 Phone and the (513) 648-4379 Phone;

3. To the extent contained on any Phone seized from the PREMISES, all records relating to violations of 18 U.S.C. § 1001, a violation involving David BRYERS and/or Shamika HEIDELBERG and occurring on or about September 28, 2021, through the present, including records and information relating to:

- a. Communications between BRYERS and HEIDELBERG related to obstructing, impeding, interfering, or influencing the investigation and judicial proceedings regarding BRYERS’ federal arrest warrant and/or wanted status.
- b. Communications from BRYERS and/or HEIDELBERG to third parties related to obstructing, impeding, interfering, or influencing the investigation and judicial proceedings regarding BRYERS’ federal arrest warrant and/or wanted status.
- c. Evidence indicating how and when the Phone was accessed or used, to determine the chronological and geographic context of access and use as it relates to the crime under investigation and the Phone’s user;

- d. Evidence indicating the Phone user's state of mind as it relates to the crime under investigation; and
 - e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.
4. For any Phone whose seizure is otherwise authorized by this warrant:
- a. evidence of who used, owned, or controlled the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the Phone was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the Phone user;
 - e. evidence indicating the Phone user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the Phone of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Phone;

- h. evidence of the times the Phone was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the Phone;
 - j. documentation and manuals that may be necessary to access the Phone or to conduct a forensic examination of the Phone;
 - k. records of or information about Internet Protocol addresses used by the Phone;
 - l. records of or information about the Phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
5. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).